UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/464,363	12/15/1999	DAVID R. IRVIN	8194-364	7440

7590 04/20/2004

Scott A. Hatfield
Myers Bigel Sibley & Sajovec
4140 PARKLAKE AVENUE
Suite 600
Raleigh, NC 27612

EXAMINER	
NOBAHAR, ABDULHAKIM	
ART UNIT	**PAPER NUMBER**
2132	10

DATE MAILED: 04/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/464,363	IRVIN, DAVID R.	
	Examiner	Art Unit	
	Abdulhakim Nobahar	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 February 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-44* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☒ Claim(s) *17-23 and 38-44* is/are allowed.

6)☒ Claim(s) *1-8,10-15 and 24-36* is/are rejected.

7)☒ Claim(s) *9, 16 and 37* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Response to Arguments

1. This communication is in response to applicant's response received on February 04, 2004.

2. Applicant's argument with respect to the use of Laubach as 102(b) reference is acknowledged and the rejection is changed to 102(e).

3. Applicant's arguments with respect to claim 1 have been fully considered but they are not persuasive.

Applicant on page 3, lines 17-18, argues that: "the HEC of Laubach is not an error check value for the unencrypted message as recited in Claim 1."

Laubach on column 8, lines 55-61, describes that the packet data (i.e., the ATM cells) are processed at the ATM cell processor which performs a Header Error Check (HEC) after they are received at the ATM network interface. The ATM cells afterward are sent for encryption to a key handler. The HEC, which is a CRC, is calculated before the encryption of the packet data as also illustrated on Fig. 4 (HEC is computed in block 404 and encryption is performed in block 406), therefore is for the unencrypted packet data (or message). Laubach also on column 8, lines 61, describes that the encryption key is selected from a table with regard to virtual path identifier (VPI) and encryption index. Thus, distribution of the encrypted data is dependent on both the VPI (destination address) and the encryption key.

4. Applicant's arguments, see page 5, lines 2-1, with respect to claim 17 have been fully considered and are persuasive. The rejection of claims 9, 16-23 and 37-44 has been withdrawn.

5. In light of the above submission the previous rejection of claims 1-8, 10-15 and 24-36 is maintained as follows.

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

2. Claims 1-8, 10-13 and 24-34 are rejected under 35 U.S.C. 102(b) as being anticipated by Laubach et al. (6,028,860) (hereinafter Laubach).

3. Regarding claims 1, 3, 5, 24 and 28, Laubach discloses a bi-directional communication system that encrypts the messages and then transmits the messages with a header error check (HEC) to an addressed destination (see, for example, column 3, lines 7-19, column 4, lines 1-7, column 8, line 51-column 9, line 15, column 17, lines 40-46 and Fig. 4). The proper encryption key is determined from a table of encryption keys for the intended destination group or an individual destination station (Fig. 4, Table 408) and a HEC (or cyclical redundancy check, CRC) is generated for each individual unencrypted message (ATM cell) by a forward error correction processor. These processes are also executed at the receiving end to determine the proper encryption key and the HEC (see, for example, Fig. 5). The combined serial stream of encrypted ATM cell-based message and its HEC is converted to a radio frequency (RF) signal. Laubach discloses that the RF signal is sent to the intended destinations according to their virtual path identifier (VPI) (see, for example, column 8, lines 29-31) via unicast (for individual station), multicast (for a group of stations), or broadcast (for all stations) on an RF channel with associated address.

4. Regarding claims 2 and 29, Laubach discloses that the destination address is a broadcast address (see, for example, column 12, line 63-column 13, line 7).

5. Regarding claims 4 and 31, Laubach discloses that the HEC is an indication of redundancy bit rate for each individual message (see, for example, column 5, lines 35-41, column 8, lines 63-65 and column 9, lines 21-26 and column 17, lines 50-56).

6. Regarding claims 6-8, 32 and 33, these claims are rejected as applied to the like elements of claim 1 above and further the following: Laubach discloses that the head-end facilitates a variety of services including prioritizing the received messages before transmission and identifying one or more receiving subscribers (see, for example, column 4, lines 1-10, column 7, lines 18-48, column 18, lines 27-46 and column 18, lines 63-column 19, line 6). The messages are sent to the respective destinations based on the specified upstream virtual connection, destination station ID and destination address. This indicates that the head-end has the capability to transmit messages without encryption for those destinations that do not require receiving encrypted messages.

7. Regarding claim 26, Laubach discloses a bi-directional system for RF signals to be transmitted between a head-end and destination station(s) according to that embodied by claim 1. Further, Laubach discloses that after the encrypted message and the accompanying error check value are received at the destination station(s), the receiving subscriber terminal unit (STU) determines the encryption key associated with the destination address, from a table similar to the process at the message transmitting end in order to decrypt the encrypted message (see, for example, column 9, lines 16-32 and Fig. 5). A header error check (HEC) is computed to be compared with the HEC received with the encrypted message. This process is executed to determine whether

an error exists or not. The decrypted message then can be sent (corresponding to the recited assigning or processing the message) to the intended computer(s) (corresponding to the recited group associated with the group encryption key).

8. Regarding claim 10, Laubach discloses that at the head-end, the type of service is determined (unicast, multicast or broadcast) and the associated encryption key is selected from a table of encryption keys (see, for example, column 8, line 55-column 9, line 15).

9. Regarding claim 11, Laubach discloses that at the receiving destination an encryption key is selected from a plurality of keys in a table, the encrypted message is decrypted and an error check value is generated for the unencrypted message in order to determine an error exists for the message or not (see, for example, column 9, lines 15-32).

10. Regarding claims 12, 13, 25 and 27, Laubach discloses a bi-directional communication system (see, for example, column 5, lines 14-21) that keeps a table of encryption keys for each destination address and for each multicast group (see column 19, lines 2-7 and lines 49-51) and that a station (corresponding to the recited user) can request resources including an encryption key from the head-end (see, for example, column 3, lines 37-44).

11. Regarding claim 30, this claim is rejected as applied to the like elements of claim 3 above.

12. Regarding claim 34, this claim is rejected as applied to the like elements of claim 12 above.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 14, 15, 35 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Laubach et al. (6,028,860) (hereinafter Laubach) in view of MacLellan et al (6,130,623) (hereinafter MacLellan).

3. Regarding claims 14, 15, 35 and 36, Laubach discloses that a table of encryption keys is kept for each destination address and for each multicast group (see column 19, lines 2-7 and lines 49-51). However, Laubach does not expressly disclose that the encryption keys are updated periodically or upon expiration of a group encryption key duration.

MacLellan teaches a system for transmitting encrypted RF signals to receiving tags that updates the encryption algorithm whenever a new generation of the system software is released (see column 6, lines 22-28). Updating encryption algorithm, naturally necessitates to update the encryption key(s), because more powerful microprocessors become available and the hackers use stronger tools.

Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to implement a mechanism for updating the encryption key(s) whenever is necessary as taught in MacLellan, in the system of Laubach, because it would make the interception and the subsequent illegal use of RF signals at least as difficult as for present day ATM cards (column 2, lines 29-32).

Allowable Subject Matter

1. Claims 9, 16 and 37 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

2. Claims 17-23 and 38-44 are allowed.

3. The following is an examiner's statement of reasons for allowance of claims 17 and 38:

4. The primary reason for the allowance of the independent claims 17 and 38 is the inclusion of the following limitations that are not found in the prior art and they are uniquely distinct features. The closest prior art is Laubach et al. (US Patent 6,028,860, hereinafter Laubach). Laubach discloses a bi-directional communication system that

computes a header error check (an error check value), encrypts the messages and then transmits the messages with the header error check to an addressed destination. Laubach also discloses that the encryption key at the transmitting end and the decryption key at the receiving end are obtained from a table based on a virtual path identifier and an encryption index. This art fails to anticipate or render the following limitation:

> "Claim 17: determining if the error check value indicates an error; and
>
> decrypting the received message using a group encryption key if the received message is directed to a broadcast address of the communication network and the error check value for the received message indicates an error."

> "Claim 38: means for determining if the error check value indicates an error; and
>
> means for decrypting the received message using a group encryption key if the received message is directed to a broadcast address of the communication network and the error check value for the received message indicates an error."

5. The dependent claims 18-23 and 39-44 are allowed because they were originally found to include a unique feature not found in the closest abovementioned art.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Abdulhakim Nobahar whose telephone number is 703-305-8074. The examiner can normally be reached on M-F 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

a.n.

Abdulhakim Nobahar
Examiner
Art Unit 2132

AN
April 13, 2004

Gilberto Barron

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100